

What is claimed is:

1 1. A key management device for managing keys, the keys being  
2 grouped into a plurality of key groups each of which is assigned  
3 to one of a plurality of reproducing devices for decrypting  
4 encrypted data to reproduce the data, the key management device  
5 comprising:

6 key storage means for storing the keys, wherein  
7 each key is associated with a node forming at least  
8 one  $N$ -layer tree structure ( $N$  is 2 or a natural number greater  
9 than 2), and

10 each key group includes keys associated with a  
11 different group of nodes, each group of nodes being a set of  
12 nodes located on a different path, in each tree structure,  
13 connecting a different node on the  $N^{\text{th}}$  layer and a node on the  
14 highest layer; and

15 encryption information generating means for, upon receipt  
16 of information designating a key group assigned to one of the  
17 reproducing devices,

18 (1) invalidating each key in the designated key  
19 group,

20 (2) selecting non-invalid keys being immediately  
21 subordinate to each invalid key from among keys in the key groups  
22 that are assigned to the other reproducing devices and each of  
23 which includes one or more invalid keys, and

24 (3) generating encryption information that includes  
25 (i) ciphertexts corresponding to a content key that is used to

encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key, and (ii) identification information for identifying the selected keys, and wherein each reproducing device stores  $N$  keys assigned thereto, selectively decrypts one of the ciphertexts that is decryptable using a key identified by the identification information to obtain the content key, and decrypts the data using the thus obtained content key to reproduce a content.

2. The key management device of Claim 1, wherein the encryption information generating means includes: a data generating unit which generates the data by encrypting the content using the content key; an invalid key accepting unit which accepts the information designating the key group assigned to the one reproducing device; a key selecting unit which invalidates each key in the designated key group, and selects the non-invalid keys being immediately subordinate on a different path to each invalid key except for the invalid key residing on the  $N^{\text{th}}$  layer; a ciphertext generating unit which generates the ciphertexts by encrypting the content key using each selected key; and a selected key list generating unit which generates a list used to identify the selected keys.

3. The key management device of Claim 2, wherein the key storage means includes a key management information

3 storage unit which stores each key's (i) identifier for  
4 identifying the key, (ii) parent key identifier for identifying  
5 its parent key being immediately superordinate to the key, (iii)  
6 key state information showing whether the key is a selected key  
7 being used to generate one of the ciphertexts, an invalid key,  
8 or a non-used key, and (iv) key data, and  
9 the invalid key accepting unit accepts identifiers for  
10 each key in the designated key group, and  
11 the key selecting unit  
12 (1) updates the key state information so as to  
13 invalidate a key of which identifier matches any of the designated  
14 identifiers, and  
15 (2) updates the key state information so as to select  
16 a key (i) of which identifier does not match any of the designated  
17 identifiers, (ii) of which parent key is invalidated, and (iii)  
18 that is neither invalidated nor selected.

1 4. The key management device of Claim 3, wherein  
2 in the key management information, the key on the highest  
3 layer has a specific value as its parent key identifier, and  
4 the key selecting unit selects the key of which parent  
5 identifier has the specific value as a selected key unless the  
6 key is invalidated.

1 5. The key management device of Claim 2, wherein the encryption  
2 information generating means further includes:  
3 a restoring key accepting unit which accepts information

4 designating a key group that has been invalidated and to be  
5 restored; and

6 a restoring unit which

7 (a) selects, from among the keys in the designated  
8 key group to be restored, a key of which parent key being  
9 immediately superordinate to the key and a brother key having  
10 the same parent key are both invalidated, and

11 (b) changes a subordinate key of the thus selected  
12 key in the designated key group to a non-used key.

1 6. The key managing device of Claim 5, wherein

2 the key storage means includes a key management information  
3 storage unit which stores, each key's (i) identifier for  
4 identifying the key, (ii) parent key identifier for identifying  
5 its parent key being immediately superordinate to the key, (iii)  
6 key state information showing whether the key is a selected key  
7 being used to generate one of the ciphertexts, an invalid key,  
8 or a non-used key, and (iv) key data,

9 the restoring key accepting unit accepts identifiers for  
10 each key in the designated key group to be restored, and

11 the restoring unit updates the key state information so  
12 as to

13 (1) select, from among keys having an identifier  
14 that matches any of the designated identifiers, (i) the key on  
15 the highest layer when its immediately subordinate key residing  
16 on a different path is currently selected, or (ii) a key on the  
17 second layer or below when its brother key having the same parent

18 key is all invalidated,

19 (2) change to a non-used key a key having an  
20 identifier that matches any of the designated identifiers and  
21 being subordinate on the same path to the thus selected key,  
22 and

23 (3) change to a non-used key a key having an  
24 identifier that does not match any of the designated identifiers  
25 and having the thus selected key as its parent key.

1 7. The key management device of Claim 2, further comprising:  
2 new key accepting means for accepting the number of  
3 reproducing devices to which a key group is newly assigned;  
4 new key generating means for generating keys which are  
5 associated with nodes forming an  $M$ -layer tree structure ( $M$  is  
6 a natural number between 2 and  $N$  inclusive); and  
7 connecting means for replacing a key on the highest layer  
8 of the newly generated tree structure with a selected key or  
9 a non-used key residing on the  $(N-M+1)^{\text{th}}$  or higher layer of the  
10 existing tree structure stored in the key recording means.

1 8. The key management device of Claim 2, further comprising  
2 recording means for recording to a recording medium the data  
3 generated by the data generating unit, the ciphertexts generated  
4 by the ciphertext generating unit, and the selected key list  
5 generated by the selected key generating unit.

1 9. The key management device of Claim 2, further comprising

transmitting means for transmitting to the plurality of reproducing devices the data generated by the data generating unit, the ciphertexts generated by the ciphertext generating unit, and the selected key list generated by the selected key generating unit.

10. The key management device of Claim 3, wherein the key management information storing unit stores the key management information every time it is updated by the key selecting unit, and the key storage means further includes a restoring unit for restoring the key management information back to its initial version or any updated version.

11. The key management device of Claim 1, wherein the key storage means stores  $L$  tree structures,  $L$  being  $2^{K+1}$  when the maximum number of key groups to be invalidated is set at  $2^K$ .

12. A recording medium to be reproduced by one of a plurality of reproducing devices each of which stores a key group, wherein each key in the key group being assigned to a node forming an  $N$ -layer tree structure ( $N$  is 2 or a natural number greater than 2) together with nodes with which keys stored in the other reproducing devices are associated, and the keys in the key group being associated with a group of nodes that is a set of nodes located on a path, in each

9 tree structure, connecting a node on the  $N^{\text{th}}$  layer and a node  
 10 on the highest layer,  
 11 the recording medium comprising:  
 12 a data area which stores data generated by encrypting a  
 13 content using a content key;  
 14 a ciphertext area which stores at least one ciphertext  
 15 generated by encrypting the content key using a selected key,  
 16 the selected key being identical to one of the keys stored in  
 17 each reproducing device except for a specifically designated  
 18 reproducing device; and  
 19 a selected key list area which stores information  
 20 identifying the selected key used for encrypting the content  
 21 key.

1 13. A reproducing device for decrypting encrypted data to  
 2 reproduce the data, the reproducing device comprising:  
 3 key group storing means for storing  $N$  keys ( $N$  is 2 or a  
 4 natural number greater than 2), wherein  
 5 the  $N$  keys are respectively associated with nodes  
 6 forming an  $N$ -layer tree structure together with nodes with which  
 7 keys stored in other reproducing devices are associated, and  
 8 the  $N$  keys are associated with a group of nodes that  
 9 is a set of nodes located on a path, in the tree structure,  
 10 connecting a node on the  $N^{\text{th}}$  layer to a node on the highest layer;  
 11 reproduction information obtaining means for obtaining  
 12 (i) the data by encrypting a content using a content key, (ii)  
 13 at least one ciphertext generated by encrypting the content key,





2 to manage keys stored in a storage area of the key management  
3 device, wherein  
4 the keys are grouped into a plurality of key groups  
5 each of which is assigned to one of a plurality of reproducing  
6 devices,  
7 each key is associated with a node forming at least  
8 one  $N$ -layer tree structure ( $N$  is 2 or a natural number greater  
9 than 2),  
10 each key group includes keys associated with a  
11 different group of nodes, each group of nodes being a set of  
12 nodes located on a different path, in each tree structure,  
13 connecting a different node on the  $N^{\text{th}}$  layer and a node on the  
14 highest layer, the key management method comprising:  
15 an accepting step for accepting information designating  
16 a key group stored in one of the reproducing devices;  
17 a key selecting step for  
18 (1) invalidating each key in the designated key group,  
19 and  
20 (2) selecting non-invalid keys being immediately  
21 subordinate to each invalid key from among keys in the key groups  
22 that are assigned to the other reproducing devices and each of  
23 which includes one or more invalid keys; and  
24 an encryption information generating step for generating  
25 encryption information that includes (i) ciphertexts  
26 corresponding to a content key that is used to encrypt the data,  
27 the ciphertexts being generated by encrypting the content key  
28 using each selected key, and (ii) identification information

29 for identifying the selected keys, and wherein  
30 each reproducing device stores  $N$  keys assigned thereto,  
31 selectively decrypts one of the ciphertexts that is decryptable  
32 using a key identified by the identification information to  
33 obtain the content key, and decrypts the data using the thus  
34 obtained content key to reproduce a content.

1 17. A key management program for use in a computer to manage  
2 keys, the keys being grouped into a plurality of key groups each  
3 of which is assigned to one of a plurality of reproducing devices,  
4 wherein  
5 each key is associated with a node forming at least  
6 one  $N$ -layer tree structure ( $N$  is 2 or a natural number greater  
7 than 2),  
8 each key group includes keys associated with a  
9 different group of nodes, each group of nodes being a set of  
10 nodes located on a different path, in each tree structure,  
11 connecting a different node on the  $N^{\text{th}}$  layer and a node on the  
12 highest layer, the program comprising:  
13 an accepting step for accepting information designating  
14 a key group stored in one of the reproducing devices;  
15 a key selecting step for  
16 (1) invalidating each key in the designated key group,  
17 and  
18 (2) selecting non-invalid keys being immediately  
19 subordinate to each invalid key from among keys in the key groups  
20 that are assigned to the other reproducing devices and each of

21 which includes one or more invalid keys; and  
22 an encryption information generating step for generating  
23 encryption information that includes (i) ciphertexts  
24 corresponding to a content key that is used to encrypt the data,  
25 the ciphertexts being generated by encrypting the content key  
26 using each selected key, and (ii) identification information  
27 for identifying the selected keys, and wherein  
28 each reproducing device stores  $N$  keys assigned thereto,  
29 selectively decrypts one of the ciphertexts that is decryptable  
30 using a key identified by the identification information to  
31 obtain the content key, and decrypts the data using the thus  
32 obtained content key to reproduce a content.

1 18. A computer readable recording medium for use in a key  
2 management device to manage keys, the keys being grouped into  
3 a plurality of key groups each of which is assigned to one of  
4 a plurality of reproducing devices, wherein  
5 each key is associated with a node forming at least  
6 one  $N$ -layer tree structure ( $N$  is 2 or a natural number greater  
7 than 2),

8 each key group includes keys associated with a  
9 different group of nodes, each group of nodes being a set of  
10 nodes located on a different path, in each tree structure,  
11 connecting a different node on the  $N^{\text{th}}$  layer and a node on the  
12 highest layer, the recording medium comprising:

13 an accepting step for accepting information designating  
14 a key group stored in one of the reproducing devices;

15           a key selecting step for  
16           (1) invalidating each key in the designated key group,  
17   and  
18           (2) selecting non-invalid keys being immediately  
19   subordinate to each invalid key from among keys in the key groups  
20   that are assigned to the other reproducing devices and each of  
21   which includes one or more invalid keys; and  
22           an encryption information generating step for generating  
23   encryption information that includes (i) ciphertexts  
24   corresponding to a content key that is used to encrypt the data,  
25   the ciphertexts being generated by encrypting the content key  
26   using each selected key, and (ii) identification information  
27   for identifying the selected keys, and wherein  
28           each reproducing device stores  $N$  keys assigned thereto,  
29   selectively decrypts one of the ciphertexts that is decryptable  
30   using a key identified by the identification information to  
31   obtain the content key, and decrypts the data using the thus  
32   obtained content key to reproduce a content.

1   19. A system comprising:  
2       a plurality of recording devices for recording encrypted  
3   data to a rewritable recording medium;  
4       a plurality of reproducing devices for decrypting and  
5   reproducing the encrypted data being recoded in the recording  
6   medium; and  
7       a key management device for managing keys, the keys being  
8   grouped into a plurality of key groups each of which is assigned

9 to the plurality of recording devices and the plurality of  
10 reproducing devices, wherein  
11 the key management device includes:  
12 key storage means for storing the keys, wherein  
13 each key is associated with a node forming at least  
14 one  $N$ -layer tree structure ( $N$  is 2 or a natural number greater  
15 than 2), and  
16 each key group includes keys associated with a  
17 different group of nodes, each group of nodes being a set of  
18 nodes located on a different path, in each tree structure,  
19 connecting a different node on the  $N^{\text{th}}$  layer and a node on the  
20 highest layer;  
21 encryption information generating means for, upon receipt  
22 of information designating a key group assigned to one of the  
23 recording devices and/or one of the reproducing devices,  
24 (1) invalidating each key in the designated key  
25 group,  
26 (2) selecting non-invalid keys being immediately  
27 subordinate to each invalid key from among keys in the key groups  
28 that are assigned to the other recording devices and/or the other  
29 reproducing devices and each of which includes one or more invalid  
30 keys, and  
31 (3) generating encryption information that includes  
32 (i) at least one ciphertext corresponding to a content key that  
33 is used to encrypt the data, the ciphertexts being generated  
34 by encrypting the content key using each selected key, and (ii)  
35 identification information for identifying the selected keys;

36 and

37 encryption information recording means for recording the  
38 thus generated encryption information to the recording medium,  
39 each recording device includes:

40 key group storing means for storing  $N$  keys, the  $N$  keys  
41 being associated with nodes located on a path, in each tree  
42 structure, connecting a node on the  $N^{\text{th}}$  layer to a node on the  
43 highest layer;

44 content key decrypting means for reading the encryption  
45 information from the recording medium, identifying a key stored  
46 in the key group storing means using the identification  
47 information, and decrypting the ciphertext being decryptable  
48 with the thus identified key to obtain the content key; and

49 content encrypting means for encrypting a content using  
50 the thus obtained content key, and record the resulting encrypted  
51 data to the recording medium, and

52 each reproducing device includes:

53 key group storing means for storing  $N$  keys, the  $N$  keys  
54 being associated with nodes located on a path, in the tree  
55 structure, connecting a node on the  $N^{\text{th}}$  layer to a node on the  
56 highest layer;

57 reproduction information obtaining means for obtaining  
58 the data generated by encrypting the content using the content  
59 key, the ciphertext generated by encrypting the content key,  
60 and the identification information for identifying the key used  
61 to encrypt the content key;

62 content key decrypting means for selecting a key identified

63 by the identification information from the keys stored in the  
64 key group storage means, and decrypting the ciphertext  
65 decryptable using the thus selected key to obtain the content  
66 key; and

67 content reproducing means for decrypting the data using  
68 the thus obtained content key to reproduce the content.

1 20. A rewritable recording medium having data generated by  
2 encrypting a content using a content key, the data being recorded  
3 by a recording device storing one of key groups, and  
4 read/reproduced by a reproducing device storing one of the key  
5 groups, wherein

6 the key groups together include keys each of which  
7 is associated with a node forming an  $N$ -layer tree structure ( $N$   
8 is 2 or a natural number greater than 2),

9 each key group includes keys associated with a  
10 different group of nodes, each group of nodes that is a set of  
11 nodes located on a different path, in the tree structure,  
12 connecting a different node on the  $N^{\text{th}}$  layer and a node on the  
13 highest layer, the recording medium comprising:

14 a ciphertext area for storing at least one ciphertext  
15 generated by encrypting the content key using a selected key,  
16 the selected key being identical to a key stored in the recoding  
17 device and a key stored in the reproducing device;

18 a selected key area for storing identification information  
19 identifying the selected key used for encrypting the content  
20 key; and

21 a data area for storing data recorded by the recording  
22 device, the data being decryptable using the content key, the  
23 content key is obtained by decrypting the ciphertext using the  
24 key that is stored in the reproducing device and selected  
25 according to the identification information.

1 21. A key management device for managing keys, the keys being  
2 grouped into a plurality of key groups each of which is assigned  
3 to one of a plurality of recording devices for recording encrypted  
4 data in a rewritable recording medium, and to one of a plurality  
5 of reproducing devices for decrypting the encrypted data recorded  
6 in the recording medium to reproduce the data, the key management  
7 device comprising:

8 key storing means key storage means for storing the keys,  
9 wherein

10 each key is associated with a node forming at least  
11 one  $N$ -layer tree structure ( $N$  is 2 or a natural number greater  
12 than 2), and

13 each key group includes keys associated with a  
14 different group of nodes, each group of nodes being a set of  
15 nodes located on a different path, in each tree structure,  
16 connecting a different node on the  $N^{\text{th}}$  layer and a node on the  
17 highest layer;

18 encryption information generating means for, upon receipt  
19 of information designating a key group assigned to one of the  
20 reproducing devices,

21 (1) invalidating each key in the designated key



22 group,

23 (2) selecting non-invalid keys being immediately

24 subordinate to each invalid key from among keys in the key groups

25 that are assigned to the other reproducing devices and each of

26 which includes one or more invalid keys, and

27 (3) generating encryption information that includes

28 (i) ciphertexts corresponding to a content key that is used to

29 encrypt the data, the ciphertexts being generated by encrypting

30 the content key using each selected key, and (ii) identification

31 information for identifying the selected keys; and

32 encryption information recording means for recording the

33 thus generated encryption information in the recording medium.

1 22. A recording device for recording encrypted data in a

2 rewritable recording medium, the recording device comprising:

3 key group storing means for storing  $N$  keys ( $N$  is 2 or a

4 natural number greater than 2), wherein

5 the  $N$  keys are respectively associated with nodes

6 forming an  $N$ -layer tree structure together with nodes with which

7 keys stored in other recording devices are associated, and

8 the  $N$  keys are associated with a group of nodes that

9 is a set of nodes located on a path, in the tree structure,

10 connecting a node on the  $N^{\text{th}}$  layer to a node on the highest layer;

11 content key decrypting means for reading the encryption

12 information from the recording medium, selecting a key stored

13 in the key group storing means using identification information,

14 and decrypting a ciphertext being decryptable with the thus

15 selected key to obtain the content key, wherein  
 16 the recording medium pre-stores encryption  
 17 information including at least the ciphertext encrypted using  
 18 the selected key and the identification information for  
 19 identifying the selected key; and  
 20 content encrypting means for encrypting a content using  
 21 the thus obtained content key, and record the resulting encrypted  
 22 data to the recording medium.